

# UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
  
1822 Stage Road  
Durham, North Carolina 27703

Case No. 18MJ345-1

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
The premises located at 1822 Stage Road, Durham, North Carolina 27703, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crimes of 18 U.S.C. §§ 2251, 2252A(a)(2)(A), and 2252A(a)(5)(B), all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §2251(a)	Production of Child Pornography
18 U.S.C. §2252A(a)(2)(A)	Distribution/Receipt of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Jerry D. Faulk, FBI Task Force Officer  
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/27/18 9:15 AM

City and state: Durham, North Carolina

  
Judge's signature

Joe L. Webster, United States Magistrate Judge  
Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Jerry D. Faulk, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I, Jerry D. Faulk, am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) in the Charlotte Division. I am currently assigned to the Child Exploitation Task Force (CETF). I was sworn in as a Special Deputy U.S. Marshal assigned to the FBI in April 2018. In December 1997, I graduated from East Carolina University with a Bachelor of Science Degree in Criminal Justice. I was hired by the Raleigh Police Department in June 1999 and graduated from the police academy in December 1999. I became a detective in November 2004 and have been assigned to General Investigations, the Robbery Unit, and the Homicide Unit. I became a member of the North Carolina Internet Crimes against Children (NCICAC) Task Force in December 2017. In my career, I have participated in several investigations involving the production, distribution, and possession of child pornography. I have also received training in the area of child pornography and child exploitation, and have observed numerous examples of child pornography as defined in 18 U.S.C. § 2256. As a TFO assigned to the FBI, I am authorized to investigate violations of federal laws and request and execute search warrants issued under the authority of the United States.

2. I am investigating a case involving child exploitation offenses. This affidavit is submitted in support of an application for warrants to search the premises located at 1822 Stage Road, Durham, North Carolina 27703 (the SUBJECT PREMISES), and the person of Alex Orlando Aguilar Guerra (the SUBJECT PERSON). The property and person to be searched are described in the following paragraphs and in Attachment A.

3. The statements in this affidavit are based on my own investigation into this matter as well as on information received from other law enforcement agents, the National Center for Missing and Exploited Children (NCMEC), and Facebook, Inc. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. This case involves violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B). Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to search the SUBJECT PREMISES and SUBJECT PERSON for contraband and evidence, fruits, and instrumentalities of these violations, more particularly described in Attachment B.

#### **STATUTORY AUTHORITY**

5. This investigation concerns alleged violations relating to the sexual exploitation of minors.

a. 18 U.S.C. § 2251(a) prohibits a person from, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in, or transporting any minor in or affecting interstate or foreign commerce, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. As described in 18 U.S.C. § 2251(e), attempts and conspiracies to violate 18 U.S.C. § 2251 fall under that section.

b. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or

facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

### **PROBABLE CAUSE**

6. In June 2017, the National Center for Missing and Exploited Children (NCMEC) received information from Facebook, Inc. regarding the distribution and receipt of child exploitation images on the Facebook social media platform. Facebook, Inc. reported that the user of the Facebook account ID 100001272827882 (Subject Account-1) was enticing two minor Facebook users, both reportedly born in 2003, to produce and send child exploitation images. According to Facebook, Inc., Subject Account-1 has a username of alex.aguilar.16906 and lists a date of birth of 09/07/1992. The account display

name is Aguilar Alex. The account also lists an email of alex.orl077@hotmail.com and phone number of (919) 760-9249. The minors will be referred to as C.G. and E.C.

7. In NCMEC CyberTipline Report 21542800, Facebook, Inc. reported that minor C.G. sent Subject Account-1 fifty-three image and video files depicting the genital and anal areas of a minor male subject. Facebook, Inc. reported the incident date as May 25, 2017. Two of the files are as follows:

“1vi3o4pba97o044c18718406\_436595543368354\_916604833\_n.jpg” is a still image that depicts the erect penis of a male subject approximately 14 years old

“bv1ry090qtc0ogosl9014468\_442055396155702\_2481466292121370624\_n.mp4” is a video file that depicts a male subject approximately 14 years inserting his finger into his anus

Facebook, Inc. reported the images were uploaded using IP address 71.69.193.186.

8. In NCMEC CyberTipline Report 21542815, Facebook, Inc. reported that minor E.C. sent Subject Account-1 five image and video files depicting the genital and anal areas of a male subject approximately 14 years old. Facebook, Inc. reported the incident date as May 25, 2017. Two of the images are as follows:

“30lg4vvsqk004k4c18716710\_226563757839241\_2114881301\_n.jpg” is a still image that depicts the penis of a male subject approximately 14 years old

“9nn85lsbdickkk4c18706087\_226565547839062\_86545510864781312\_n.mp4” is a video file that depicts a male subject approximately 14 years old inserting his finger into his anus

Facebook, Inc. reported that both of these images were uploaded using IP address 71.69.193.186.

9. In NCMEC CyberTipline Report 21542777, Facebook, Inc. reported that Subject Account-1 uploaded an image on May 28, 2017 and then another image on May 29, 2017. The images are as follows:

“evql2ucrzm04ckwo18741676\_437247943303114\_85614390\_n.jpg” is a still image that depicts a male subject approximately 12-13 years old with his genital and anal areas exposed

“ca8ysq23i7swocs818788712\_437973386563903\_2070588353\_n.jpg” is a still image that depicts the anus of a male subject approximately 12-13 years old

Facebook, Inc. reported that both of these images were uploaded using IP address 71.69.193.186.

10. In NCMEC CyberTipline Report 22575646, Facebook, Inc. reported that Subject Account-1 enticed minors C.G. and E.C. to produce and send child

exploitation images. In the report to NCMEC, Facebook, Inc. included excerpts from sexually explicit communications<sup>1</sup> between Subject Account-1 and the minors. The chats between Subject Account-1 and C.G. are dated from May 12, 2017 to June 7, 2017. The chats between Subject Account-1 and E.C. are dated from May 18, 2017 to May 26, 2017. According to Facebook, IP address 71.69.193.186 was associated with Subject Account-1 on July 18, 2017. The chats include the following excerpts:

C.G. & Subject Account-1:

May 25, 2017:

Subject Account-1	Do you have school
C.G.	<i>Yes from</i>
C.G.	<i>From 1 to 5</i>
Subject Account-1	What grade are you in?
C.G.	<i>7 seventh</i>
Subject Account-1	That's great
Subject Account-1	Are you 14 years old
Subject Account-1	??
C.G.	<i>I'm 13</i>

May 26, 2017:

C.G.	<i>I sent you plenty</i>
Subject Account-1	haha
C.G.	<i>And naked</i>
Subject Account-1	delete them

May 30, 2017:

Subject Account-1	I want a video where you masturbate your little butt but I know you wouldn't dare
C.G.	<i>Fine but later</i>
Subject Account-1	Mmm

---

<sup>1</sup> In the NCMEC report the communications are reflected in Spanish and have been translated into English by Facebook, Inc.



C.G.

*And how do I masturbate my behind?*

---

E.C. & Subject Account-1:

May 18, 2017:

Subject Account-1	And how old are you
E.C.	<i>Guess</i>
E.C.	<i>Are</i>
E.C.	<i>Old</i>
E.C.	<i>You</i>
E.C.	<i>How</i>
E.C.	<i>old are you</i>
Subject Account-1	24
E.C.	<i>12 years old</i>
Subject Account-1	God
Subject Account-1	You are a kid
Subject Account-1	Heheh

May 26, 2017:

Subject Account-1	I want to see it sticking up
E.C.	<i>And from outside</i>
Subject Account-1	?
E.C.	[image reported by Facebook, Inc. as a child exploitation image]
Subject Account-1	It's up
E.C.	[image reported by Facebook, Inc. as a child exploitation image]
E.C.	<i>Yes</i>
E.C.	<i>I want to see yours</i>
Subject Account-1	Open up your little butt baby
Subject Account-1	I want to see it good
E.C.	<i>Oh god</i>
Subject Account-1	What
E.C.	<i>Now it's your turn</i>
E.C.	<i>You</i>
E.C.	<i>I already sent to you</i>

11. NCMEC CyberTipline Report 22575646 also documents that the user of Facebook account ID 100018319993329 (Subject Account-2), with display name Orlando Aguilar and email orlando090792@outlook.com, communicated<sup>2</sup> on Facebook with C.G on June 22 and 23, 2017. Facebook, Inc. reported that Subject Account-1 is linked by machine cookies to Subject Account-2. An excerpt follows:

C.G. & Subject Account-2:

June 22, 2017:

C.G.	[image reported by Facebook, Inc. in CyberTipline Report 22513931 depicting the anal area of a male subject approximately 12-14 years old]
Subject Account-1	Mmmm

12. A search warrant was served on Facebook, Inc. on October 9, 2018 requesting account records for Subject Account-1 and Subject Account-2 from April 1, 2017 to October 3, 2018. The records were received on October 11, 2018. The records indicate that the accounts for Subject Account-1 and Subject Account-2 were both disabled by Facebook on July 18, 2017. The records corroborate the information described above, specifically the communications with C.G. and E.C.

13. A review of the Facebook records revealed that Subject Account-1 and Subject Account-2 communicated with other minors.

---

<sup>2</sup> In the NCMEC report the communications are listed in Spanish and have been translated into English by Facebook, Inc.

14. Subject Account-1 communicated with minor D.G. from April 23, 2017 to June 3, 2017. During their communication, minor D.G. told Subject Account-1 that he was 16 years old. Subsequently, minor D.G. sent a profile image of what he purported to be his bare buttocks to the user of Subject Account-1. Then, on April 24, 2017, the user of Subject Account-1 sent a purported image of himself to minor D.G. That image is as follows:

“image-1443134622405618” is a still image that depicts a penis with ejaculate

15. Subject Account-1 communicated with minor W.R. from May 29, 2017 to June 7, 2017. During their communications, minor W.R. told Subject Account-1 he was 17 years old. Minor W.R. sent multiple images he purported to be himself to Subject Account-1. Two of the images are as follows:

“image-110126899581029” is a still image that depicts a hand holding the penis of a male subject

“image-108738946386491” is a still image that depicts the penis of a male subject

16. Subject Account-2 communicated with W.R. from June 27, 2017 to July 17, 2017. Minor W.R. sent multiple images he purported to be himself to Subject Account-2 from June 27, 2017 to July 17, 2017. Two of the images are as follows:

“image-133541940572858” is a still image that depicts a male subject approximately 17 years old in a sitting position, nude with his penis and genitals exposed

“image-133542217239497” is a still image that depicts the anal and genital area of a male subject approximately 17 years old

17. Subject Account-1 communicated with G.U. from April 6, 2017 to June 10, 2017. G.U. appears to be approximately 15 years of age. G.U. sent multiple images to Subject Account-1 from April 6, 2017 to June 10, 2017. Two of the images are as follows:

“image-290383038074134” is a still image that depicts a male subject approximately 15 years old in a standing position, nude with his penis and genitals exposed

“image-290383071407464” is a still image that depicts a hand holding the penis of a male subject approximately 15 years old

18. Records for the IP address 71.69.193.186 were subpoenaed on July 20, 2017. The IP address resolved to 1822 Stage Road, Durham, NC 27703 and the subscriber was Deysi Aguilar. The lease for the IP address started on October 30, 2016 and ended on July 21, 2017.

19. According to records from Facebook, Inc., Subject Account-1 was registered under the display name “Alex Aguilar” from June 5, 2010 to July 18,

2017, and Subject Account-2 was registered under the display name "Orlando Aguilar" from June 20, 2017 to July 18, 2017.

20. Research of open sources indicated a subject named Alex Orlando Aguilar Guerra with a date of birth of 9-7-1992 lives at the SUBJECT PREMISES.

21. A search of North Carolina Division of Motor Vehicles (DMV) records conducted on November 6, 2018 revealed that an individual named Alex Orlando Aguilar Guerra with DOB: 09/07/1992 resides at the SUBJECT PREMISES. The photograph for this individual was compared to images of the user for Subject Account-1 and Subject Account-2. Based on the visual comparison, Alex Orlando Aguilar Guerra, the SUBJECT PERSON, was the user of the two accounts. DMV records also reveal that a 2006 Honda Civic is registered to the SUBJECT PERSON.

22. Additional research of open sources showed a male subject named Alex Orlando Aguilar registered as a voter with North Carolina Board of Elections on February 20, 2018 and listed the SUBJECT ADDRESS as his address.

23. The SUBJECT ADDRESS is located within Durham County. Research of open source information for Durham County property records showed the residence was conveyed to Deysi Aida Aguilar and Alex O. Aguilar Guerra on March 9, 2016.

24. Surveillance was conducted at the SUBJECT PREMISES on October 24, 2018 at approximately 12:30 pm. Several vehicles belonging to a subject named Orlando Aguilar Rosales were parked at the residence. The Honda Civic registered to the SUBJECT PERSON was not present.

25. Surveillance was conducted at the residence again on November 7, 2018 at approximately 11:00 pm. Again, there were several vehicles parked at the residence including the Honda Civic registered to the SUBJECT PERSON.

**BACKGROUND ON COMPUTERS, CHILD PORNOGRAPHY, AND THE INTERNET**

26. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know the following about computer-related child exploitation crimes:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital images can be produced using a variety of devices including digital cameras, laptop/desktop computers, and mobile devices. Unlike traditional photography, digital photography typically allows a user to easily and inexpensively take and store large quantities of images. In fact,

once a device is purchased there is no expense associated with capturing images.

c. With today's technology, digital images can be easily transferred between a user's devices and among individuals. Internet Service Providers enable users to connect to the Internet through a variety of means such as cable, Wi-Fi, and cellular service. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. Child pornography can be transferred via email, MMS text message, mobile messaging applications, cloud storage services, and webpage bulletin boards to anyone with access to a computer and the Internet. Individuals interested in the sexual exploitation of children use technology to exchange child pornography with each other and to transfer their child pornography between their devices.

d. Individuals interested in the sexual exploitation of children also use technology to target minors, interact with minors, and entice minors to produce child pornography. This is often accomplished through the use of social networking applications such as Facebook, Instagram, Kik Messenger, Musical.ly, and LiveMe.

e. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it to any one of the mentioned media storage devices. Media storage devices can easily be concealed and carried on an individual's person. Mobile devices, such as smartphones, are also often carried on an individual's person.

f. Cloud storage services are further changing how electronic data is stored. These services, such as Dropbox, Box, and OneDrive enable a user to store data on remote services and access it on any of their computers by using installed applications/software. A user can also access their data via an Internet Browser from any computer with an Internet connection. Cloud storage services provide a convenient way to share data with others. This is



accomplished by creating a hyperlink to the selected data or simply providing the username and password to the account. Recently, this has become a particularly popular way to share child pornography. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer or external media in most cases.

g. Mobile devices are hand-held computers that can transfer media through multiple methods – cellular signal, Wi-Fi, Bluetooth, and near field communication (NFC). In addition, mobile devices are commonly set to backup automatically when connected to a computer. Individuals have been known to plug their mobile devices into computers causing data to be backed up to the computer without even realizing that this data transfer is occurring. Mobile devices can also be set to sync automatically with Cloud storage and paired devices. For example, an individual using Google Pictures or iCloud Photo Library may have images taken using a mobile device automatically backup to cloud storage and pushed out to, or “synced,” with their other computer devices.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, “bookmarked” files). Digital information can also be retained

unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, application data, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the internet (*e.g.*, tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (*e.g.*, prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE,  
TRANSPORT, RECEIVE, POSSESS, AND ACCESS WITH INTENT TO  
VIEW CHILD PORNOGRAPHY**

27. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, transport, receive, possess, and access with intent to view child pornography:

a. Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals often collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain any hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area and/or password protected mobile device. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Further, individuals who produce child pornography are less likely to delete it because, unless they

have distributed it, they are likely the only ones who possess it. Therefore, produced child pornography files are unique and all the more valuable.

e. Importantly, evidence of such activity often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

28. Based on the following, I believe that the SUBJECT PERSON, who resides at the SUBJECT PREMISES, likely displays characteristics common to individuals who produce, transport, receive, possess, and access with intent to view child pornography. For example, the user of the subject Facebook accounts

solicited/received child pornography on multiple dates, solicited/received child pornography on from multiple minors, and uploaded child pornography to his Facebook account.

### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

29. As described in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES and on the SUBJECT PERSON. One form in which records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of all electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

30. I submit that if a computer or storage medium is found at the SUBJECT PREMISES and on the SUBJECT PERSON, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so

because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

31. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the



evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data

that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

32. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

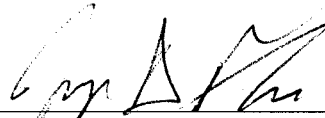
a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

### CONCLUSION

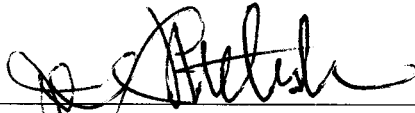
33. Based on the forgoing, I believe there is probable cause that the federal criminal statutes cited herein have been violated, and that contraband, evidence, fruits and instrumentalities of these offenses, more particularly described in Attachment B, are located at the SUBJECT PREMISES, more particularly described in Attachment A, and on the SUBJECT PERSON. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES and the SUBJECT PERSON, authorizing the seizure and search of the items described in Attachment B.

Respectfully submitted,



Jerry D. Faulk  
Task Force Officer  
Federal Bureau of Investigation

Subscribed and sworn to before me on 27th day of November 2018. 9:15 AM



Joe L. Webster  
United States Magistrate Judge  
Middle District Of North Carolina

## ATTACHMENT A

---

### Premises to Be Searched

The premises to be searched is a residence located at 1822 Stage Road in Durham, North Carolina 27703 which is within the Middle District of North Carolina. The residence is a single story house with a red brick exterior, blue window shutters and white front door. The number "1822" is displayed on a black mailbox at the entrance of the driveway beside Stage Road.



## ATTACHMENT A

---



## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of

- malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
  - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - f. evidence of the times the COMPUTER was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - i. records of or information about Internet Protocol addresses used by the COMPUTER;
  - j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content.



3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
  - a. Records, information, and items referencing or revealing the occupancy or ownership of 1822 Stage Road, Durham, North Carolina 27703;
  - b. Records and information referencing or revealing the use or ownership of Facebook accounts 100001272827882 and 100018319993329, email accounts alex.ori077@hotmail.com and orlando090792@outlook.com, and phone number (919) 760-9249;
  - c. Records and information revealing sexual interest in minors;
  - d. Records and information revealing or referencing communications/interactions of an illicit sexual nature with minors and records and information revealing or referencing the identity of any such minors;
  - e. Records and information referencing or revealing the sexual exploitation of children, including communication between individuals engaged in the distribution and production of child pornography;

- f. Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography;
  - g. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage.
- 6. During the course of the search, photographs of the residence may be taken to record the condition thereof and/or the location of items therein.
- 7. During the course of the search warrant, law enforcement officers may press the fingers (including thumbs) of Alex Orlando Aguilar Guerra (DOB: 09/07/1992) to the fingerprint sensor of any device recovered pursuant to this search warrant for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.